

241901077

PONSURABHI V

Ex.No:1

Date:01/08/2025

CAPTURE FLAGS-ENCRYPTION CRYPTO 101

AIM:

To capture the various flags in Encryption Crypto 101 in TryHackMe platform.

ALGORITHM:

1. Access the Passive reconnaissance lab in TryHackMe platform using the link below-
<https://tryhackme.com/r/room/encryptioncrypto101>
2. Click Start AttackBox to run the instance of Kali Linux distribution.
3. Solve the crypto math used in RSA.
4. Find out who issued the HTTPS Certificate to tryhackme.com
5. Perform SSH Authentication by generating public and private key pair using ssh-keygen
6. Perform decryption of the gpg encrypted file and find out the secret word.

OUTPUT:

The screenshot shows a dark-themed interface for a crypto challenge room. At the top, there's a navigation bar with 'Learn > Encryption - Crypto 101'. Below it is a header with a lock icon, the title 'Encryption - Crypto 101', a subtitle 'An introduction to encryption, as part of a series on crypto', and stats like '45 min' and '132,562'. A progress bar at the bottom indicates 'Room completed (100%)'. The main area contains 12 tasks, each with a green checkmark and a description: Task 1 (What will this room cover?), Task 2 (Key terms), Task 3 (Why is Encryption important?), Task 4 (Crucial Crypto Maths), Task 5 (Types of Encryption), Task 6 (RSA - Rivest Shamir Adleman), Task 7 (Establishing Keys Using Asymmetric Cryptography), Task 8 (Digital signatures and Certificates), Task 9 (SSH Authentication), Task 10 (Explaining Diffie Hellman Key Exchange), Task 11 (PGP, GPG and AES), and Task 12 (The Future - Quantum Computers and Encryption). Each task has a dropdown arrow to its right.

```
root@ip-10-10-146-227:~# python3
Python 3.6.9 (default, Nov 25 2022, 14:10:45)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 118613842 % 9091
3565
>>> 
```

241901077

PONSURABHI V

```
root@ip-10-10-162-62:~# python3 "/root/Tools/Password Attacks/john/ssh2john.py"
idrsa.id_rsa > idrsa.txt
root@ip-10-10-162-62:~# ls
CTFBuilder  Downloads      idrsa.txt      Pictures   Rooms      thinclient_drives
Desktop     idrsa.id_rsa  Instructions  Postman    Scripts   Tools
root@ip-10-10-162-62:~# john --wordlist=/usr/share/wordlists/rockyou.txt idrsa.txt
Note: This format may emit false positives, so it will keep trying even after finding a
possible candidate.
Warning: detected hash type "SSH", but the string is also recognized as "ssh-opencl"
Use the "--format=ssh-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
delicious      (idrsa.id_rsa)
```

```
root@ip-10-10-162-62:~# gpg --import tryhackme.key
gpg: /root/.gnupg/trustdb.gpg: trustdb created
gpg: key FFA4B5252BAEB2E6: public key "TryHackMe (Example Key)" imported
gpg: key FFA4B5252BAEB2E6: secret key imported
gpg: Total number processed: 1
gpg:          imported: 1
gpg:          secret keys read: 1
gpg:          secret keys imported: 1
root@ip-10-10-162-62:~# gog message.gpg

Command 'gog' not found, but there are 17 similar ones.

root@ip-10-10-162-62:~# gpg message.gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
      "TryHackMe (Example Key)"
root@ip-10-10-162-62:~# gpg --decrypt message.gpg
gpg: encrypted with 1024-bit RSA key, ID 2A0A5FDC5081B1C5, created 2020-06-30
      "TryHackMe (Example Key)"
You decrypted the file!
The secret word is Pineapple.
```

RESULT:

Thus, the various flags have been captured in Encryption Crypto 101 in TryHackMe platform.